Results for " (((key)<in>metadata) <and> ((update)<in>metadata))<and> ((encryption)<... "
Your search matched 43 of 1993012 documents. You selected 25 items.

e-mail

Display Format: ○ Citation ● Citation & Abstract

Article Information View: 1-25 | Viev

» Download Citations

Citation & Abstract

ASCII Text

» Learn more

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

1. Practical key distribution schemes for channel protection
Yu-Lun Huang; Shieh, S.-P.W.; Jian-Chyuan Wang
Computer Software and Applications Conference, 2000. COMPSAC 2000. The 24th A
International
2000
Page(s): 569-574
Digital Object Identifier 10.1109/CMPSAC.2000.884782
Summary: The paper presents three key distribution schemes for channel protection.
proposed schemes, encryption keys of the ordered programs can be distributed to the
subscribers efficiently and securely. In these schemes, for key updates,.....
AbstractPlus | Full Text: PDF IEEE CNF

2. Selecting the Advanced Encryption Standard
Burr, W.E.
Security & Privacy, IEEE
Volume: 1 Issue: 2 Mar-Apr 2003
Page(s): 43- 52
Digital Object Identifier 10.1109/MSECP.2003.1193210
Summary: The USA National Institute of Standards and Technology selected the Adv
Standard, a new standard symmetric key encryption algorithm, from 15 qualifying algo
also made efforts to update and extend their standard crypto.....
AbstractPlus | References | Full Text: PDF IEEE JNL

3. A study on secure wireless networks consisting of home appliances
Nakakita, H.; Yamaguchi, K.; Hashimoto, M.; Saito, T.; Sakurai, M.
Consumer Electronics, IEEE Transactions on
Volume: 49 Issue: 2 May 2003
Page(s): 375- 381
Digital Object Identifier 10.1109/TCE.2003.1209528
Summary: We propose a security system for a wireless home network, regarding whi
need not be aware of configuration of IP address or wireless LAN protocol type. This s
that a server manages a connectivity of each appliance to the wir.....
AbstractPlus | Full Text: PDF IEEE JNL

4. Improved LKH for batch rekeying in multicast groups
Pegueroles, J.; Rico-Novella, F.; Hernandez-Serrano, J.; Soriano, M.
Information Technology: Research and Education, 2003. Proceedings. ITRE2003. Inte
Conference on
11-13 Aug. 2003
Page(s): 269- 273
Digital Object Identifier 10.1109/ITRE.2003.1270619
Summary: Storage, delivery and update of cryptographic keys are the most importan
multicast security. Traditionally a centralized trusted third party called the key server (k
these actions. Different works have been presented th.....
AbstractPlus | Full Text: PDF IEEE CNF

5. Efficient state updates for key management
Pinkas, B.
Proceedings of the IEEE
Volume: 92 Issue: 6 June 2004
Page(s): 910- 917
Digital Object Identifier 10.1109/JPROC.2004.827355
Summary: Encryption is widely used to enforce usage rules for digital content. In man
content is encrypted using a group key which is known to a group of users that are allc
content. When users leave or join the group, the group key m.....

AbstractPlus | References | Full Text: PDF IEEE JNL

6. Reconfigurable key management for broadcast encryption
Mihaljevic, M.J.
Communications Letters, IEEE
Volume: 8 Issue: 7 July 2004
Page(s): 440- 442
Digital Object Identifier 10.1109/LCOMM.2004.832774
Summary: A novel approach for the cryptographic keys management in the broadcas
a conditional access control is proposed. It employs the reconfiguration concept, and i
collection of the underlying structures - at each instant.....

AbstractPlus | References | Full Text: PDF IEEE JNL

7. Efficient key distribution schemes for secure media delivery in pay-TV systems
Yu-Lun Huang; Shiuhpyng Shieh; Fu-Shen Ho; Jian-Chyuan Wang
Multimedia, IEEE Transactions on
Volume: 6 Issue: 5 Oct. 2004
Page(s): 760- 769
Digital Object Identifier 10.1109/TMM.2004.834861
Summary: To provide secure media delivery in pay-TV systems, a large number of m
exchanged for key updates in the conventional key distribution schemes. This is ineffic
when the client side (set-top box) uses a smart card with limit.....

AbstractPlus | References | Full Text: PDF IEEE JNL

8. Scalable, Server-Passive, User-Anonymous Timed Release Cryptography
Chan, A.C.-F.; Blake, I.F.
Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE Internati
on
10-10 June 2005
Page(s): 504-513
Digital Object Identifier 10.1109/ICDCS.2005.72
Summary: We consider the problem of sending messages into the future, commonly k
release cryptography. Existing schemes for this task either solve the relative time prob
uncontrollable, coarse-grained release time (time-lock puzzle approa.....

AbstractPlus | Full Text: PDF IEEE CNF

9. Provably unbreakable hyper-encryption in the limited access model
Rabin, M.O.
Theory and Practice in Information-Theoretic Security, 2005. IEEE Information Theory
19-19 Oct. 2005
Page(s): 34-37
Digital Object Identifier 10.1109/ITWTPI.2005.1543953
Summary: Encryption is a fundamental building block for computer and communicatic
Existing encryption methods depend for their security on unproven assumptions. We p
model, the limited access model for enabling a simple and practic.....

AbstractPlus | Full Text: PDF IEEE CNF

10.
Improving the security of SNMP in wireless networks
Otrok, H.; Mourad, A.; Debbabi, M.; Assi, C.
Wireless Networks, Communications and Mobile Computing, 2005 International Confe
Volume: 1 13-16 June 2005

Page(s): 198- 202 vol.1
Digital Object Identifier 10.1109/WIRLES.2005.1549409
Summary: Simple network management protocol (SNMP) is widely used for monitorii
computers and network devices on wired and wireless network. SNMPv1 and v2 do nc
when managing agents. Three very important security features (aut.....

AbstractPlus | Full Text: PDF IEEE CNF

11. Performance analysis of multicast key backbone for secure group communicatic
Rung-Hung Gau
Communications Letters, IEEE
Volume: 10 Issue: 7 July 2006
Page(s): 555-557
Digital Object Identifier 10.1109/LCOM.2006.224418
Summary: In this paper, we propose and analyze a multicast key backbone for secure
communications. When a group member joins or leaves the multicast group, the syste
and distribute encryption keys to assure that only active members could .....

AbstractPlus | Full Text: PDF IEEE JNL

12. A Multi-Seed Key Distribution Scheme Based on PE
Yumin Xie; Feng Shi; Muhammad Kamran
Intelligent Control and Automation, 2006. WCICA 2006. The Sixth World Congress on
Volume: 2 0-0 0
Page(s): 6763-6766
Digital Object Identifier 10.1109/WCICA.2006.1714393
Summary: The key problem of securing multicast is to generate, distribute and update
encryption key (SEK). A group key distribution scheme utilizing a polynomial expansio
(M-PE) is proposed. Its operation is demonstrated by using multi.....

AbstractPlus | Full Text: PDF IEEE CNF

13. A New Forward-Secure Signcryption Scheme
Yin Xin-Chun; Chen Jue-Wei; Wang Cai-Mei
Communications, Circuits and Systems Proceedings, 2006 International Conference o
Volume: 3 25-28 June 2006
Page(s): 1615-1617
Digital Object Identifier 10.1109/ICCCAS.2006.284982
Summary: Signcryption scheme combines digital signature and encryption functions.
signcryption, once the long-term private key is compromised, all signatures even those
the honest signer before the compromise, will not be trustworthy.....

AbstractPlus | Full Text: PDF IEEE CNF

14. Special-Purpose Hardware in Cryptanalysis: The Case of 1,024-Bit RSA
Willi Geiselmann; Rainer Steinwandt
Security & Privacy, IEEE
Volume: 5 Issue: 1 Jan.-Feb. 2007
Page(s): 63-66
Digital Object Identifier 10.1109/MSP.2007.20
Summary: For efficiency, we should implement cryptographic subsystems with short k
estimating minimal key lengths is a rather involved and complicated process - especia
with long life cycles and limited update capabilities. In .....

AbstractPlus | References | Full Text: PDF IEEE JNL

15.
The Secure Field Bus (SecFB) Protocol - Network Communication Security for s
Process control
Swaminathan, P.; Padmanabhan, K.; Ananthi, S.; Pradeep, R.
TENCON 2006. 2006 IEEE Region 10 Conference
14-17 Nov. 2006
Page(s): 1-4
Digital Object Identifier 10.1109/TENCON.2006.344134
Summary: This paper describes a protocol by which network security can be included
Fieldbus systems. The protocol makes use of the 56-bit DES cipher for data encryptio

a scheme for symmetric key exchange and automatic key update.....

AbstractPlus | Full Text: PDF IEEE CNF

16. A Scalable Secure Multicast System
Zhao Yu Chi; Atwood, J.W.
Electrical and Computer Engineerng, 2007. CCECE 2007. Canadian Conference on
22-26 April 2007
Page(s): 982-985
Digital Object Identifier 10.1109/CCECE.2007.251
Summary: Multicast is an efficient way to distribute data to multiple receivers simultan
security, scalability, and group management issues still prevent the wide deployment c
transmission. In this paper, we will present a Scal.....

AbstractPlus | Full Text: PDF IEEE CNF

17. The Biometrics Grid: A Solution to Biometric Technologies
Goth, G.
Distributed Systems Online, IEEE
Volume: 8 Issue: 9 Sept. 2007
Page(s): 1-1
Digital Object Identifier 10.1109/MDSO.2007.4370097
Summary: It might appear that the technology industry just discovered encryption-key
2007. Since the beginning of the year, data-security product vendors, enterprise custo
standards bodies have embraced efforts to standardize methods fo.....

AbstractPlus | Full Text: PDF IEEE JNL

18. Confidential and Secure Broadcast in Wireless Sensor Networks
Shaheen, J.; Ostry, D.; Sivaraman, V.; Jha, S.
Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th Ir
Symposium on
3-7 Sept. 2007
Page(s): 1-5
Digital Object Identifier 10.1109/PIMRC.2007.4394560
Summary: Wireless sensor networks need broadcast for operations such as software
queries, and command dissemination. Alongside ensuring authenticity of the source ai
the broadcast data secret is vital in certain applications su.....

AbstractPlus | Full Text: PDF IEEE CNF

19. Group Key Update Method for Improving RC4 Stream Cipher in Wireless Sensor
Chuan-Chin Pu; Wan-Young Chung
Convergence Information Technology, 2007. International Conference on
21-23 Nov. 2007
Page(s): 1366-1371
Digital Object Identifier 10.1109/ICCIT.2007.277
Summary: To secure the wireless sensor network (WSN) for data transmission, RC4
able to provide the advantages of fast performance and simplicity in resource constrai
Since RC4 stream cipher is a symmetry key encryption algori.....

AbstractPlus | Full Text: PDF IEEE CNF

20. Optimal Communication Complexity of Generic Multicast Key Distribution
Micciancio, D.; Panjwani, S.
Networking, IEEE/ACM Transactions on
Volume: 16 Issue: 4 Aug. 2008
Page(s): 803-813
Digital Object Identifier 10.1109/TNET.2007.905593
Summary: We prove a tight lower bound on the communication complexity of secure
distribution protocols in which rekey messages are built using symmetric-key encryptic
generators, and secret sharing schemes. Our lower bound .....

AbstractPlus | References | Full Text: PDF IEEE JNL

21. Secured route optimization in mobile IPv6 wireless networks in terms of data int

Mehdizadeh, A.; Khatun, S.; Borhanuddin, M.A.; Raja Abdullah, R.S.A.; Kurup, G.
Computer and Communication Engineering, 2008. ICCCE 2008. International Confere
13-15 May 2008
Page(s): 643-646
Digital Object Identifier 10.1109/ICCCE.2008.4580683
Summary: Route optimization (RO) in mobile IPv6 (MIPv6) provides a mobile node (M
communicate with correspondent node (CN) directly, using shortest possible path and
inefficient triangle routing. MIPv6 uses return routability procedure to authe.....

AbstractPlus | Full Text: PDF IEEE CNF

22. Distributed Access Control For XML Document Centric Collaborations
Rahaman, M.A.; Roudier, Y.; Schaad, A.
Enterprise Distributed Object Computing Conference, 2008. EDOC '08. 12th Internatio
15-19 Sept. 2008
Page(s): 267-276
Digital Object Identifier 10.1109/EDOC.2008.31
Summary: This paper introduces a distributed and fine grained access control mecha
encryption for XML document centric collaborative applications. This mechanism also
to simultaneously protect the confidentiality of a document a.....

AbstractPlus | Full Text: PDF IEEE CNF

23. A Secure Key Management Scheme for Wireless and Mobile Ad Hoc Networks U
Based Approach: Proof and Correctness
Boukerche, A.; Yonglin Ren; Samarah, S.
Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE
Nov. 30 2008-Dec. 4 2008
Page(s): 1-5
Digital Object Identifier 10.1109/GLOCOM.2008.ECP.353
Summary: Security plays an important role in today's information technology, particula
and mobile environments due to the lack of pre-deployed infrastructure and the unsuita
centralized management. Since the encryption technique has be.....

AbstractPlus | Full Text: PDF IEEE CNF

24. Generic Construction of Certificate-Based Encryption
Lu, Yang; Li, Jiguo; Xiao, Junmo
Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for
18-21 Nov. 2008
Page(s): 1589-1594
Digital Object Identifier 10.1109/ICYCS.2008.11
Summary: In Eurocrypt 2003, Gentry introduced a new public key encryption paradigr
certificate-based encryption (CBE) to overcome the drawbacks of the conventional PK
based encryption (IBE). CBE provides an efficient implicit certific.....

AbstractPlus | Full Text: PDF IEEE CNF

25. A New Approach to Securing Broadcast Data in Sensor Networks
Poornima, A.S.; Amberker, B.B.
Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for
18-21 Nov. 2008
Page(s): 1998-2001
Digital Object Identifier 10.1109/ICYCS.2008.451
Summary: Wireless Sensor Networks have a wide spectrum of applications ranging fr
war fare. Applications like network query, software updates, time synchronization and
management demand for broadcast security. In these applications if.....

AbstractPlus | Full Text: PDF IEEE CNF

View: 1-25 | View Search Resi

Help Contact Us Privacy &